A VANET privacy protection scheme based on fair blind signature and secret sharing algorithm

Xiaoliang Wang, Shuifan Li, Shujing Zhao & Zhihua Xia

To cite this article: Xiaoliang Wang, Shuifan Li, Shujing Zhao & Zhihua Xia (2017) A VANET privacy protection scheme based on fair blind signature and secret sharing algorithm, Automatika, 58:3, 287-294, DOI: 10.1080/00051144.2018.1426294

To link to this article: https://doi.org/10.1080/00051144.2018.1426294

Published online: 09 Feb 2018.

Submit your article to this journal

View related articles

View Crossmark data

Taylor & Francis
Taylor & Francis Group

REGULAR PAPER

A VANET privacy protection scheme based on fair blind signature and secret sharing algorithm

Xiaoliang Wang [a], Shuifan Li [a], Shujing Zhao [a] and Zhihua Xia [b]

aSchool of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan, China; bSchool of Computer & Software, Nanjing University of Information Science & Technology, Nanjing, China

ABSTRACT

Vehicular ad hoc network (VANET) is a traffic application of wireless sensor network, which is also a new mobile ad hoc networks composed of vehicle nodes, roadside units, service providers and other components. In VANET, data is transmitted by the wireless channel, which is subject to potential threat like information leak and data attack due to the openness and sensitivity of the auto organization network itself. How to ensure the identity privacy and trusted communication in VANETs is the key issue to be solved urgently. The existing work usually uses authentication mechanism, but the user's privacy disclosure is inevitable during the authentication process. Some anonymous authentication schemes have been proposed to solve the problem of privacy disclosure regardless of considering anonymity abuse. However, anonymity abuse is also severe in VANET. In view of the above problems, this paper proposes a scheme based on fair blind signature and secret sharing algorithm. By security analysis and experiment, the scheme has been proved to be higher anonymity and higher efficiency.

1. Introduction

VANET (vehicular ad hoc network) is a kind of mobile ad hoc network, which has many features such as multi-hop, self-organization and rapid change of network topology. It establishes a temporary multi-hop autonomous network through the wireless communication between vehicles and road infrastructures, which can ensure the information exchange such as the speeds and the locations. Generally, VANET is composed of several parts: (1). OBU (on board unit). (2). RSU (roadside unit). (3). AC (authentication centre) and (4). SP (service provider). VANET communication mainly includes vehicle to vehicle and vehicle to infrastructure. Because of the self-organization of the vehicular network, the vehicle node should be used as not only the wireless communication node to transmit its own messages, but also a wireless router node to relay messages to the other nodes in order to achieve the long-distance messages transmission. At the same time, a vehicle is also a sense node to perceive common traffic information and vehicle information such as position, speed, direction and driving condition and so on. RSU is the roadside base station that provides indirect communication among vehicles and between vehicles and administration department. It can also provide Internet access service for vehicles. As an information service provider of Internet, SP can provide many Internet services for vehicles [1,2].

When the network is deployed in large-scale, because of the rapid change of network topology, the delay of communication and the lack of trust mechanism, there exists a series of problems, such as message authentication delay, channel instability and bandwidth shortage. Therefore, the design of highly efficient and reliable authentication scheme is the research hotspot of the VANET [3,4]. At the same time, the information of the user's identity and location is important and sensitive in the process of communication, so it has to ensure anonymity as well as reliability. In recent years, a lot of researchers had put forward some kinds of anonymous authentication schemes. However, there are some weaknesses in these studies. Some studies do not consider the single fault, some studies only provide the anonymity between different vehicles but not between vehicles and RSUs, some ignore the necessity of tracking after the anonymity is abused by malicious users. These weaknesses make proposed schemes unsuitable for the requirements of VANET.

In view of the above problems, this paper presents a self-organized anonymous authentication and tracking scheme based on the fair blind signature and secret sharing algorithm, focusing on identity information protection and communication anonymity.

2. Related work

In recent years, a variety of authentication schemes are proposed in the literatures. Ma et al. [5] combine smart card and password authentication technology to design

---

CONTACT Xiaoliang Wang ✉ fengwxl@163.com

a secure authentication scheme, which can resist the offline password guessing and denial of service attacks and provides forward secrecy and ensures user anonymity. Wang et al. [6] consider the trade-off between security and privacy and put forward an anonymous two-factor authentication scheme based on the basic evaluation index. Based on Kim-Kim two-factor authentication technology, a method [7] is proposed to enhance the program efficiency without additional communication and computational overhead while increasing security ability.

In VANET, the privacy information like user identity and location is important and sensitive in the communication process. System should ensure not only the authentic identity but also prevent privacy from leaking [2]. The previous schemes protecting VANET privacy focus on the identity of the anonymous authentication. Common techniques used in studies include group signature scheme [8–10], ring signature scheme [11], ID-based signature scheme [12–16], blind signature [17] or mess-up technology and so on [18–21].

Sun et al. [8] and Guo et al. [9] earlier used Boneh group signature technology for in-vehicle communications. Calandriello et al. [10] point out that the computational overhead and length of the group signature in the signature generation and verification process are much larger than the general public key infrastructure (PKI) digital signature schemes (such as ECDSA), so schemes using the kind of signature for in-vehicle safety are inefficient. Following researchers wanted to improve the high overhead and security risks of the group signature. Among them, some researchers resorted to use ring signature scheme to achieve the desired objectives. Ring signature is similar to a simplified group signature scheme and it uses rules to form a ring, which has anonymity feature. For example, Zhang et al. [11] propose a privacy-preserving authentication protocol based on ring signature without bilinear pairings in VANETs. It achieves effective privacy protection and authentication mechanisms and also reduces the computational overhead of signature generation process because of discarding the complex operation of bilinear pairings. There are some researchers who focus on using the identity-based signature (IBS) to implement identity-based anonymous authentication such as Sun et al. [12], Li et al. [13], Jinila and Komathy [14], Zhu et al. [15] and He et al. [16]. Among these international researchers, Sun et al. [12] are relatively early researchers who paid attention to this problem. They used zero-knowledge proof and threshold secret sharing algorithm to design an anonymous identity authentication scheme based on signatures. PPAS [15] uses IBS based on bilinear pairings to solve anonymous authentication issues not only between OBUs but also between the RSUs and OBUs. In addition, in order to achieve conditional privacy

and authentication purposes. He et al. [16] design a similar identity-based signature. But because it is based on elliptic curve algorithm without bilinear pairings operation, it has less computational overhead and more safe. Proxy Blind Signature Scheme (PBSS) [17] proposes a signature scheme based on blind signature and proxy multi-signature certification technology, which solves authentication problems between the nodes. The use of two signature technologies realizes the on-board authentication interactivity and improved communication safety. Experimental results show that PBSS can better meet the on-board node mobility and complexity and the authentication efficiency has good performance.

Other VANET anonymous authentication schemes use different kinds of obfuscation techniques, such as pseudonym and mix technology and so on. VSPN [18] uses bilinear mappings and proxy re-encryption mechanism to design a pseudonym authentication for automotive networks. Van den Berg et al. [19] propose a vehicle-based certificate-selection method for enhancing the privacy in VANETs, in which vehicles share numbers of certificates. Each vehicle is able to detect and identify the certificates used by neighbours and then it can choose a used certificate for its own safety communication. This method makes the certificate not unique to achieve anonymous authentication enhancing privacy. In addition, k-anonymity is also used in this field. K-anonymity means unless there are k-1 data that are released at the same time the k-user can be disclosed. Chen et al. [20] propose a query-aware location privacy scheme based on p-sensitive and k-anonymity for road networks, which puts all the k users as an anonymous entity in a certain area and authority uses the optimized queries to determine a specific entity. The study of Cabellero-Gil et al. [21] is also based on k anonymous algorithm, but it takes into account the tracking after the anonymous abuse. Theoretical and experimental analysis shows that it can improve the effectiveness of the tracking. LESPP [22] uses lightweight symmetric encryption and message authentication code (MAC) to generate signature and can quickly verify regenerated MAC signature with a low memory overhead, but fails to consider the problem of single point failure. 2FLIP [23] is based on dispersed trusted authority using several lightweight terminals' hash signature and MAC to rapidly sign and authenticate nodes. It has a strong repudiation, and also can conditionally track the real information of vehicle. But the whole tracking process is under the control of a certain trusted authority, also without considering the single point failure.

Above studies are based on a coarse-grained classification. In reality, researcher needs to integrate multiple technologies to complete a scheme. For example, based on hash chain, bilinear pairings, IBS and pseudonym PASS [24] optimizes certificate revocation list in pseudonym
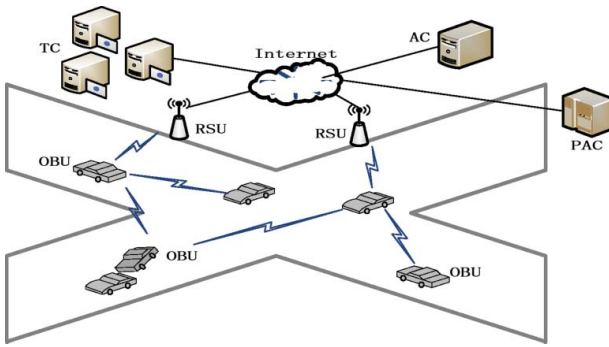
Figure 1. Basic network structure model.

authentication and certificate renewal process, which significantly reduces the system overhead of the scheme.

As we mentioned above, there are also many weaknesses existing in current studies, such as single point failure, anonymity abuse and so on. So we propose a novel mechanism to improve them.

3. System model and research objectives

3.1. Basic network structure

The network model used in this project mainly includes three types of entities as illustrated in Figure 1.

(1) Vehicle entity, called V. Set its true identity as IDV, pseudonym as $IDPV$. Each of vehicle entities includes the on-board unit and common communication unit, such as sensor input unit, wireless communication unit, processor and hardware security unit. OBU stores the information of the vehicle, such as ID, license plate number, related vehicle properties and other information, which is not easy to be changed.

(2) RSU, which consists of radio frequency controller, network communication module, power module and microwave transceiver module, is responsible for the signal and data transmission, encoding and decoding, decryption and so on. Compared to the OBU node, with higher storage and forwarding capabilities, it is responsible for communication with not only vehicle units but also Internet.

(3) Trusted centre. It mainly contains AC, PAC (pseudonym authentication centre) and TC (tracking centre).

3.2. Research objectives

The main features of the program have:

(1) The separation of anonymous authentication and tracking of vehicles. Vehicle's pseudonym for the certification application is jointly produced by the certification centre and the vehicle, which can detect any fraud and forgery attack.

(2) Distributed pseudonym tracking. Not a single TC is in charge of all the tracking information that avoids the single point failure and improves the robustness of the scheme. At the same time, the possibility of collusion is very low if the number of compromised tracking centres is less than a certain threshold.

(3) TC does not need to store pseudonym certificate and the relation of pseudonym and ID, which reduces storage and search overhead of the TC.

(4) Privacy protection. For an honest and law-abiding vehicle node in the VANET, its identity privacy will be protected as well as the identity of the illegal vehicle is to be tracked if anonymity abuse happens.

4. Anonymous authentication scheme based on fair blind signature and secret sharing

4.1. Basic process of scheme

(1) Vehicle V is registered at AC, and it is verified and signed by AC.

(2) The vehicle V applies for pseudonymous certificate from PAC, and it is verified by PAC before pseudonym is issued.

(3) V safely communicates with other vehicles and RSUs via pseudonym certificate.

(4) TC uses secret sharing algorithm in a tracking group to keep the private key from the process of verification and pseudonym creation. If anonymity abuse and other violations of the law happen, other vehicles are able to request PAC, TC to track the pseudonym of the relevant malicious vehicle.

(5) TC convenes members of the tracking group to restore the true identity of the malicious vehicle, and revoke pseudonym and punish this vehicle.

4.2. The detailed algorithm

This scheme is based on the idea of fair blind signature and secret sharing algorithm, taking into account both aspects of privacy protection and the tracking of anonymous abuse. IDV is the pivotal information for vehicle V, which is kept as a secret. In mutual communication, vehicle V uses the signed pseudonym rather than true identity to anonymously interact with other vehicles and RSU node. This requires a unique signature for each vehicle node, and the signature must be derived from the trusted third party. In this signature algorithm, the PAC works as the trusted third party to issue a reliable pseudonym certificate that does not disclose IDV of V. At the same time, if an anonymous abuse happens in the vehicle communication process, the victim can put forward a tracking appeal, and then the tracking group will convene the

relevant members to restore the identity information of the malicious vehicle.

4.2.1. Pseudonym issue based on a fair blind signature

Pseudonym issue mainly includes the following phases

Phase 1 Initialization

The vehicle nodes, AC, PAC, TC, respectively, generate the corresponding public key and private key. V generates IDV's public key (NV, eV) and private key dV, which can be used for a long time. AC generates public key (NAC, eAC) and private key dAC. PAC generates public key $(NPAC, ePAC)$ and private key d PAC that will be frequently updated. TC generates public key (NTC, eTC) and private key dTC. AC, PAC and TC open public key and the vehicle is loaded with the pre-installed public keys of AC, PAC and TC.

Phase 2 Vehicle registration phase

The main steps of this phase are as follows:

(1) V registers at AC.

V secretly sends $IDV\|n\|SV\|CertV$ to AC. SV is the signature that V signs for the above data, which is denoted as $(IDV\|n)^{dV} \bmod / NV$, where n is the number of applications for pseudonyms and IDV contains the information of vehicle identity.

(2) AC verifies and issues pseudonym.

AC checks the signature $(IDV\|n)^{dV} \bmod / NV$. If successful, AC agrees to issue a pseudonym and return $IDAC\|IDV\|ts\|SAC$ to V, where ts is a time stamp of validity period and SAC is the signature $[(IDAC\|IDV\|ts)^{dAC} \bmod NAC]^{eV} \bmod NV$, which AC signs for the above data.

(3) V verifies AC's signature.

V extracts and decrypts $[(IDAC\|IDV\|ts)^{dAC} \bmod NAC]^{eV}$ $\bmod NV$ and gets $(IDAC\|IDV\|ts)^{dAC} \bmod NAC$. Then, V verifies AC's signature. If successful, it selects random numbers Ai, Bi ($1 \le i \le n$) and transmits the blind value $Bi^{eAC}Ai$ to AC.

(4) AC calculates $Ci = (Bi^{eAC}Ai \bullet (i\|IDV\|ts))^{dAC}$, $Di = ((i\|IDV\|ts)^{eTC})^{dAC}$ and returns the result to V.

(5) V verifies $Di^{eAC} = (i\|IDV\|ts)^{eTC}$. If successful, it gets rid of blind factor and gets $Ei, 1 = Ci/Bi$ and $Ei, 2 = (Ei, 1^{eTC})/Di$. Assuming the pseudonym ID is $IDPVi = Ai \bullet (i\|IDV\|ts)\|Ai^{eTC}$. V sends $(IDAC\|IDPVi\|Ei, 1\|Ei, 2\|ePVi\|NPVi\|SPVi)^{ePAC}$ to PAC, $1 \le i \le n$, where $SPVi$ is the signature that V signs to get temporary private key $dPVi$.

(6) PAC verifies the signature and issues certificate.

PAC checks the signature of the V. If successful, it extracts $IDPVi$ and gets $Ai \bullet (i\|IDV\|ts)$, Ai^{eTC}, $Ei, 1$ and $Ei, 2$. Then, it verifies whether $Ei, 1^{eAC} = (Ci/Bi)^{eAC} = (Ai \bullet (i\|IDV\|ts)^{dAC})^{eAC} = Ai \bullet (i\|IDV\|ts)$ and $Ei, 2^{eAC} = (Ei, 1^{eTC}/Di)^{eAC} = \frac{(Ai \bullet (i\|IDV\|ts))^{eTC}}{(i\|IDV\|ts)^{eTC}} = Ai^{eTC}$. If successful, PAC sends $Certpvi = IDPAC\|IDPVi\|ts\|ePVi\|NPVi\|SPAC$ to V.

4.2.2. Anonymous communication

After the completion of the pseudonym issue, the vehicle will use pseudonym during anonymous communication. Assume the vehicle as V. V selects $Certpvi$ ($1 \le i \le n$) from n pseudonym certificates and combines temporary private signing key $dPVi$ with the message to be sent to form anonymous message set Mj ($1 \le i \le m$, m is the number of messages in this message set), and then V broadcasts the message set to nearby area. After receiving the message set, nearby vehicle will use the public key information of the initialization phase to verify the validity of signature. If successful, nearby vehicle will accept it or opt to continue broadcasting to next neighbours. If unsuccessful, nearby vehicle will discard it as an invalid message set.

4.2.3. Threshold sharing

After the completion of the signing, TC is in charge of saving the private key dTC. In order to avoid single point of failure, the secret sharing scheme is utilized. In the scheme, the dTC is not stored in the TC for a long time, but kept in a tracking group. System allocates the private key dTC to m tracking members and at least $n(n \le m)$ members are needed to work together to recover the private key information. Secret sharing process of dTC is as follows:

(1) After the completion of the signing, TC determines m peers as the tracking members from the decentralized TC group. Assume these members are $T1, T2, T3.....Tm$, the threshold value is $n(n \le m)$, namely at least n tracking members are needed to restore information.

(2) Assume finite field $GE(f)$, in which f is a prime number and $f > m$. TC distributes the private key to m tracking members. To ensure these tracking members share the private key and at least n tracking members are needed to restore information, system selects $n - 1$ independent factors in the finite field $a1, a2, ai..., an - 1$ ($0 \le ai \le f$). At the same time, it defines random polynomial $f(x) = \sum_{j=0}^{n-1} ajx^j = a0 + a1x + \cdots + an - 1x^{n-1}$, where $a0$ is the key dTC to be shared.

(3) TC randomly selects different values i, every i meets ($1 \le i \le m$). Calculate $(dTC)i = f(i)$ $\bmod f$, then distribute the shared $(dTC)i$ and the corresponding i to the tracking group. After

completion of the distribution of the private key, TC clears the private key information.

4.2.4. Distributed tracking illegal vehicle

When the anonymous illegal behaviour happens, other vehicles can put forward the request to the tracking group to find the malicious vehicle. According to the known pseudonym certificate, the group members can join to recover the pseudonym to the real information of illegal vehicle, so that the tracking function takes effect.

The main processes are as follows:

(1) When receiving an illegal message submitted by a victim vehicle, PAC first gets pseudonym certificate $CertPV$ from the message and checks whether the message time stamp is effective. If the verification is successful, PAC will collect data-set and send the pseudonym tracking request q to the tracking group.

(2) TC and PAC verify whether the signature $CertPV$ is valid. If successful, they extract $IDPV$ from $CertPV$. Then, TC gathers tracking group members together, and distributes the message $IDPV \| q$ among members. Because the recovery of the private key will need at least n members, TC randomly selects n members from the tracking group who share the private key. These n members can provide their shared fragment $(xi, yi) = (i, dTCi)$. Using the Lagrange interpolation formula, TC can obtain a polynomial $f(x) = \sum_{i=1,i\neq j}^{n} yi \prod_{i\neq j} \frac{x - xj}{xi - xj}$. From the above process, TC can obtain $dTC = f(0) = \sum_{i=1,i\neq j}^{n} yi \prod_{i\neq j} \frac{-xj}{xi - xj}$.

5. Security analysis

5.1. The anonymity of the scheme

In the process of communication, AC, PAC and other ordinary vehicles in VANET cannot discover the corresponding relationship between the pseudonym of a vehicle and its real identity. After the private key information is distributed to the tracking group, the TC in the signing process will be no longer involved in any subsequent communication. Other vehicles can verify a certain blind signature, but cannot know the true identity of corresponding vehicle, which ensure a good protection for privacy.

(1) For AC, because the parameters Ai, Bi are randomly generated and only stored in the vehicle V, even if AC obtains IDV, $Bi^{eAC} Ai$, Ci, Di, and ts information, it is impossible to deduce parameter Ai so it does not calcu-

late $IDPVi = Ai \bullet (i\|IDV\|ts)\|Ai^{eTC}$. Therefore, AC cannot get the corresponding relationship between identity and pseudonym.

(2) For PAC, because the dTC is the unique information of the TC, even if PAC has obtained $IDPVi$, $Ei, 1$, $Ei, 2$, ts, $NPVi$, $ePVi$ or other relevant information, without the private key of TC it is impossible to obtain the value of the parameter Ai from Ai^{eTC} by $Ei, 1$, $Ei, 2$ and $IDPVi$. Therefore, PAC is unable to relate the pseudonym with true identity of vehicles.

(3) For other vehicles in the VANET, even if they have gained $IDPVi$, ts, $ePVi$ and $NPVi$ information, without the private key dTC of TC, they cannot extract any relevant information from a certain pseudonym because the difficulty of decryption of Ai^{eTC} is equivalent to the attack to algorithm RSA, which is infeasible in the computation.

5.2. Traceability of the scheme

Only with the help of more than n tracking members, the scheme can restore the true identity via the pseudonym, which ensures anonymity as well as tracking function. Vehicle node registers in AC, then PAC and TC combine to deal with pseudonym, so the true identity of the vehicle has some link with the system, which exists in the subsequent communication. By distributing the private key information to different tracking members, the scheme can avoid the single track centre failure but is easy to track the illegal vehicles.

5.3. The authentication security of the scheme

The scheme can satisfy the security of authentication process. In the process of pseudonym application, every message will carry the corresponding signature, which means the messages without signature will not be accepted. This can ensure the effectiveness of authentication and prevent common attack. The difficulty that vehicles, PAC or other attackers want to forge signatures or pseudonyms to implement fraud are equivalent to the factorization of large numbers.

(1) Anti-forgery attack

In the process of V application for pseudonym from PAC, if another vehicle V' wants to forge $V's$ pseudonym, it needs to forge the parameters $Ei, 1$ and $Ei, 2$, in which $Ei, 1$ meets $Ei, 1^{eAC} = Ai \cdot (i\|IDV'\|ts)$, $Ei, 2$ meets $Ei, 2^{eAC} = Ai^{eTC}$. Because the dAC is a secret of AC, V' cannot get it, and the calculation of $Ei, 1$ and $Ei, 2$ is infeasible, so V' cannot pass the verification of PAC. At the same time, because of the existence of time stamp ts, it is more difficult to forge a pseudonym.

(2) Tamper resistance attack

In the process of certification, the information that V sends to AC cannot be tampered by AC. The reason is as follows. If the false identity information is added to the blind signature, the blind signature in authentication phase cannot be passed when V calculates whether $Di^{eAC} = (i\|IDV\|ts)^{eTC}$. On the other hand, the information that V sent to PAC has been attached with the signature of PAC and verified by AC, so V itself cannot change the signature information. The difficulty to tamper a signature is also equivalent to the difficulty of the decomposition of large factor.

(3) Effectiveness of authentication

In the process of pseudonym application, V is verified and signed by AC, and use attained signature to obtain pseudonym certificate from PAC. The whole process needs mutual authentication. In the process of communication, the vehicle is accepted by the other vehicles using this pseudonym certificate. If an external attacker wants to cheat others, it has to simultaneously forge the signature of V and AC, which is infeasible in computation.

5.4. The robustness of the scheme

(1) The registration at AC, the pseudonym issue at PAC and tracking with the assistance of TC are separated, so AC and PAC are not able to have tracking capability. Even if AC, PAC are compromised, the vehicle's true identity will not be disclosed.

(2) In secret sharing phase of the scheme, the private key dTC is split and distributed to m tracking members. If an attacker gets less than n shares of the private key, it cannot restore the polynomial $f(x)$. Also for conspiracy attack, less than n TCs cannot conspire to calculate the private key dTC. In the legal recovery process, the private key d TC can also be recovered even if loss of some shares occurs. In practical application, we can reasonably set the values of parameters m and n to improve the security, so the scheme can have strong robustness.

6. Experiment and result analysis

To verify the effectiveness of the proposed scheme, simulation experiment is carried out. Experiment uses C++ language and is based on visual studio 2012 platform of Windows7 system with 2.6 GHZ i5 processor and 4G memory. The experimental data-set is generated using Thomas Brinkhoff road network [25] widely recognized by the mobile data management industry. Oldenburg traffic network (5 km*5 km) is taken as the input to generate mobile data-set and communication node objects as illustrated in Figure 2.
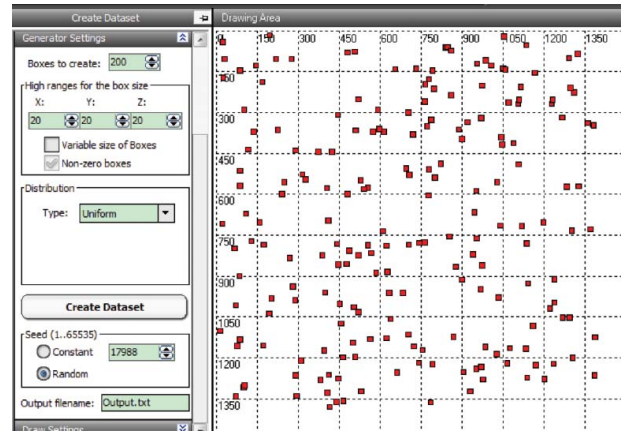

Figure 2. The communication node.

According to the definition of data packet format of security standard IEEE 1609.2 [26] for VANET, the definition of pseudonym message format is as follows.

MID is the message identifier, which defines the message type in a pseudonym period. MData is the information carried by the effective data including the relevant information of the vehicle, such as vehicle speed, location, direction, etc. TS is the time stamp which records the time of message creation to prevent invalid packet and message replay attack. Sign is the signature for the above three data items. CertPV is the pseudonym certificate, TTL is the survival time which defines the termination of messages transmission to prevent the infinite spread of message.

Consider a communication cycle using a pseudonym certificate. If all messages in the transmission have a pseudonym certificate, communication overhead is too large. However, if only the front single message includes pseudonym certificate instead of the behind message, if communication channel problem occurs, for example, the receiver does not successfully receive a certain message, the other messages in this communication cycle are unable to be verified. Assume y is the number of the whole messages in pseudonymous communication period, Z is the number of messages carrying pseudonym. The experiment uses message receiving ratio model of communication channel provided by paper [10], namely $Precv(d) = -0.04d + 1/7 \times \sin(\pi/125\,d) + 1$, where $Precv$ is message receiving rate and d is the message transmission distance. Message authentication success rate is defined as $Pauth = 1 - (1 - Precv)^z$. Figure 3

Table 1. Vehicle message format.

Parameter	Default value
MID	2 B
MData	100 B
TS	4 B
Sign	136 B
CertPV	698 B
TTL	1 B
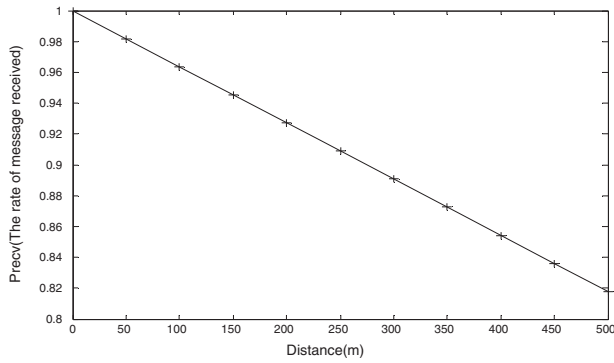
Figure 3. The impact of d.

Figure 4. The effect of different $Precv$ and z.

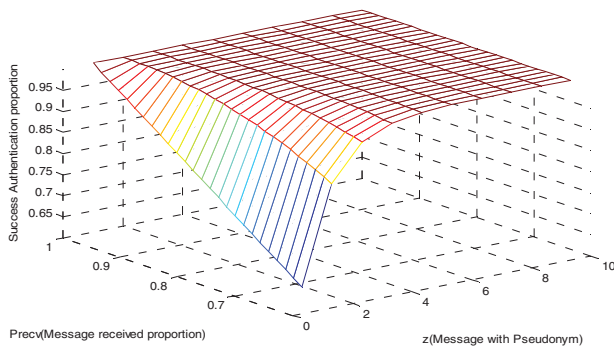**Figure 5.** The average of message.

illustrates the impact of the message transmission distance to the message-receiving rate. When the distance increases, the message-receiving rate is reduced.

Figure 4 illustrates the relationship between message transmission distance d, the number of messages of a pseudonym carrying Z and the success authentication rate $Pauth$. With the decreasing of the d, the success receiving rate increases. When d is fixed, with the increasing of the number of pseudonym carrying messages, the success authentication rate increases accordingly. From this picture, we can learn message success authentication rate is more than 90% when $Precv \geq 95$ % ($d \leq 150\,m$), $z \geq 4$, so we select the number of messages of a pseudonym $z = 4$, which is able to meet the authentication requirement for most of the conditions.

6.1. Performance analysis

Table 2 compares some algorithms, PBSS [17], LESPP [22] and 2FLIP [23] in anonymity, authentication and traceability fields. PBSS [17] adopts the distributed

Table 2. The comparison of different schemes.

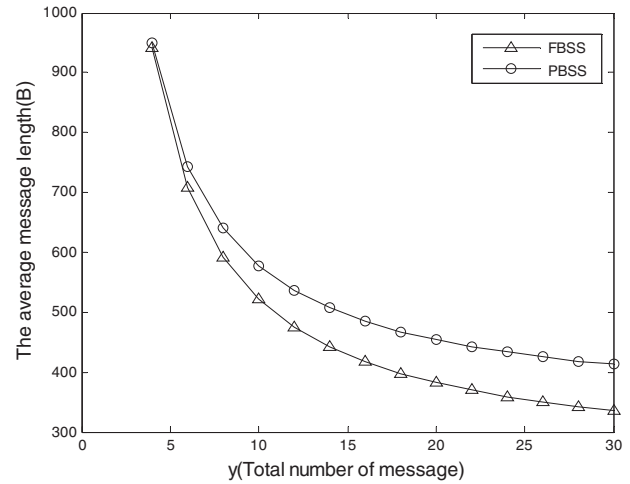|	Table column head			
Attributes	PBSS	LESPP	2FLIP	FBSS
Integrity	✓	✓	✓	✓
Authentication	✓	✓	✓	✓
Anonymity	✓	✓	✓	✓
Strong privacy protection	✗	✓	✓	✓
Conditional tracking	✗	✓	✓	✓
Distributed tracking	✗	✗	✗	✓

proxy blind signature, which can avoid forgery attacks and meet authentication security, but never considers tracking of the abuse of anonymous. The whole tracking process of LESPP [22] and 2FLIP [23] is highly dependent on a certain trusted authority, without considering the single point failure and tracking abuse of the trusted authority.

6.2. Communication and storage overhead

The scheme PBSS [17] needs three phases: the signature authorization, proxy signature and signature verification. Each message in the process of signature needs to carry a pseudonym certificate. Compared with PBSS, the number of the interaction in the pseudonym issue phase is reduced to two rounds. At the same time, it is unnecessary that all the information carry pseudonym certificate in the signature process. In this experiment, we set the number of messages in a communication cycle as 400. Define the average length of the message by $len = (z\,941 + (y - z))/y$. When $z = 4$, guaranteeing the success rate $Pauth \geq 90\%$, the relationship between the average message size and the total number of messages in a cycle is as follows.

From Figure 5 we can see that when the total number of periodical messages increases, the average length of the message decreases. In the case of plenty of pseudonym messages, both schemes can reduce the overhead. However, our scheme is better than PBSS.

7. Conclusion

Aiming to protect privacy in VANET, this paper proposes a secure scheme based on fair blind signature and threshold secret sharing. This scheme has good effect of anonymity, low storage overhead and high efficiency, and can also track the anonymous abuse cases, which can effectively prevent the illegal vehicle from attacking. It can meet the double requirements of

anonymous authentication and tracking abuse of ano-
nymity in VANET.

ORCID

Xiaoliang Wang http://orcid.org/0000-0002-6229-4601
Shuifan Li http://orcid.org/0000-0001-7439-4688
Shujing Zhao http://orcid.org/0000-0003-1965-1252

References

[1] Lu H, Li J. Privacy-preserving authentication schemes for vehicular ad hoc networks: a survey. Wirel Commun Mob Comput. 2016;16(6):643–655.

[2] Patil V, Patil PS. Secured and privacy preserving navigation for VANET. Int J Elect Electro Res. 2015;3(2):305–309.

[3] Sun YP. Research on privacy preserving technologies in VANET [dissertation]. Changsha: National University of Defense Technology; 2010. Chinese.

[4] Mejri MN, Ben-Othman J, Hamdi M. Survey on VANET security challenges and possible cryptographic solutions. Veh Commun. 2014;1(2):53–66.

[5] Ma C-G, Wang D, Zhao S-D. Security flaws in two improved remote user authentication schemes using smart cards. Int J Commun Syst. 2014;27(10):2215–2227.

[6] Wang D, Wang P, He D. Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment. IEEE Trans Dependable Secur Comput. 2014;12(4):428–442.

[7] Wang D, Wang N, Wang P, et al. Preserving privacy for free: efficient and provably secure two-factor authentication scheme with user anonymity. Inf Sci (Ny). 2015;321(5):162–178.

[8] Sun X, Lin X, Ho P-H. Secure vehicular communications based on group signature and ID-based signature scheme. In: Connery S, Brown G, editors. IEEE International Conference on Communications. Glasgow (Scotland): IEEE Press; 2007. p. 1539–1545.

[9] Guo J, Baugh J, Wang S. A group signature based secure and privacy-preserving vehicular communication framework. In: Tonguz K, Wisitpongphan N, Bai F, et al. editors. 2007 Mobile Networking for Vehicular Environments. Anchorage (AK): IEEE Press; 2007. P. 103–108.

[10] Calandriello G, Papadimitrators P, Hubaux J-P. Efficient and robust pseudonymous authentication in VANET. In: Holfelder W, Santi P, editors. Proceedings of the 4th ACM International Workshop on Vehicular Ad Hoc Networks; 2007 Sep 10. Montréal (QC):ACM SIGMOBILE; 2007. p. 19–28.

[11] Zhang J. Xu YCM. A novel and efficient privacy-preserving authentication protocol in VANETs. Int J Digit Content Technol its Appl. 2012;6(9):157–164.

[12] Sun J, Zhang C, Zhang Y, et al. An identity-based security system for user privacy in vehicular ad hoc networks. IEEE Trans Parallel Distrib Syst. 2010;21(9):1227–1239.

[13] Li J, Lu H, Guizani M. ACPN: a novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs. IEEE Trans Parallel Distrib Syst. 2015;26(4):938–948.

[14] Jinila YB, Komathy K. An efficient authentication scheme for Vanet using Cha Cheon's ID based signatures. Indian J Appl Res. 2014;2(6):106–109.

[15] Zhu H, Liu T, Wei G, et al. PPAS: privacy protection authentication scheme for VANET. Cluster Comput. 2013;16(4):873–886.

[16] He D, Zeadally S, Xu B, et al. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. IEEE Trans Inf Forensics Secur. 2015;10(12):2681–2691.

[17] Tian X, Qiang S. Research of an authentication scheme based on the proxy blind signature scheme for the vehicular ad-hoc networks. Bull Sci Technol (Chinese). 2012;28(10):170–173.

[18] Chim TW, Yiu SM, Hui LCK. VSPN: VANET based secure and privacy-preserving navigation. IEEE Trans Comput. 2014;63(2): 510–524.

[19] van den Berg S, Zhang E, Pietrowicz T. Blend-in: a privacy-enhancing certificate-selection method for vehicular communication. IEEE Trans Veh Technol. 2009;58(9):5190–5199.

[20] Chen J, Xu H, Zhu L. Query-aware location privacy model based on p-sensitive and k-anonymity for road networks. In: Fengjuan W, editor. International Workshop on Internet of Things; 2012 Aug 17–19. Changsha: Springer Verlag Press; 2012; p. 157–165.

[21] Caballero-Gil C, Molina-Gil J, Hernandez-Serrano J, et al. Providing k-anonymity and revocation in ubiquitous VANETs. Ad Hoc Networks. 2016;36(1):482–494.

[22] Wang M, Liu D, Zhu L, et al. LESPP: lightweight and efficient strong privacy preserving authentication scheme for secure VANET communication. Computing. 2016;98(7):685–708.

[23] Wang F, Xu Y, Zhang H, et al. 2FLIP: a two-factor lightweight privacy-preserving authentication scheme for VANET. IEEE Trans Veh Technol. 2016;65(2):896–911.

[24] Sun Y, Lu R, Lin X, et al. An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications. IEEE Trans Veh Technol. 2010;59(7):3589–3603.

[25] Brinkhoff T. A framework for generating network-based moving objects. Geoinformatica. 2002;6(2):153–180.

[26] IEEE-SA Standardization. IEEE trial-use standard for wireless access in vehicular environments – security services for applications and management messages. New York: IEEE-SA Standards Board; 2006. IEEE Std No. 1609.2-2006.